Human Technology Institute

UTS

Artificial Intelligence

Corporate Governance Snapshot

Artificial Intelligence (AI) promises to deliver great benefit to society and organisations. To harness these significant opportunities in increasingly complex external and internal environments, stewards and leaders need effective governance systems that can support responsible innovation.

This snapshot provides early insights into the ways AI is being used by Australian organisations, the key risks that can arise to employees, consumers and citizens, and a summary of current obligations and duties that may apply.

The AI Corporate Governance Program is an initiative of the UTS Human Technology Institute (HTI) and aims to broaden understanding of corporate accountability and governance in the use of AI. HTI is grateful to our major philanthropic project funder Minderoo Foundation, and project advisory partners KPMG, Gilbert + Tobin and Atlassian. This summary of current obligations and directors' duties draws upon legal research produced by Gilbert + Tobin.

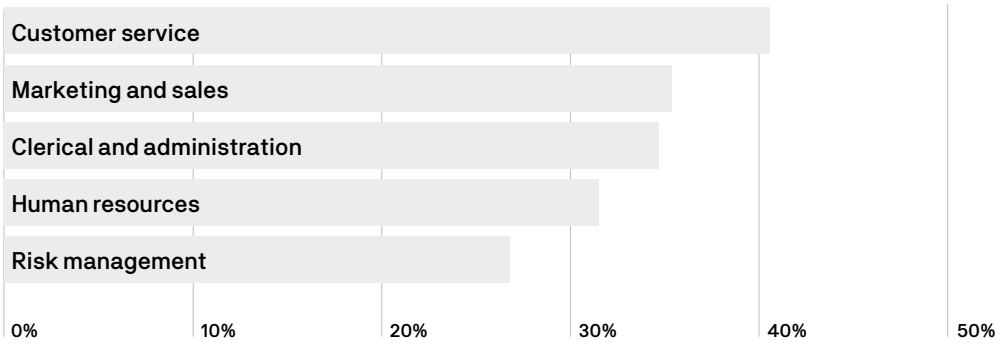
For more information on this program of work, future events, or to access the latest research findings please contact us at hti@uts.edu.au

Australian organisations are significant users of AI

Research conducted by HTI in December 2022 found **two-thirds** (66%) of Australian business decision makers[1] surveyed were either already using – or are planning to use – AI systems in their operations. This finding is broadly consistent with trends in local uptake from 2021[2].

The **top five** operational areas prioritised for AI deployment were: customer service; marketing and sales; clerical and administrative; and human resources and risk management (Figure 1). Respondents cited internal process efficiencies (62%), increased productivity (54%) and better customer experience (51%) as the greatest expected benefits.

Figure 1: Top five use cases for AI in Australian organisations (2022)



66%
of Australian business decision makers were either already using – are planning to use – AI systems.

Potential harms to individuals from top use cases

Rapid adoption of AI by Australian organisations can deliver significant commercial and social benefit, however without adequate guardrails, a range of potential harms can be created or amplified for people as citizens, workers and consumers (Table 1). **Three out of the top five** operational areas prioritised by Australian organisations for AI use (customer service, marketing and sales, and human resources) directly impact experiences of consumers, employees, or potential employees.

Table 1: Examples of potential harms to employees, consumers and citizens

Provision of misleading information or advice	AI is used to provide information or advice to consumers which is misleading or deceptive, e.g. product rankings and recommendations which are incorrect or misleading.
Unfair treatment	Where an AI-enabled system may unfairly result in poorer service provision, higher costs, or obstruct ability to exercise choice or consumer rights, e.g. AI-enabled web interfaces which deliberately obstruct the ability to cancel subscriptions or confuse and manipulate purchase decisions.
Unlawful discrimination or exclusion from basic services	One or more users are denied access to a basic service or entitlement, or experience systematically worse treatment based on a protected attribute, e.g. AI-enabled job application screening unfairly excluding people with a disability.
Psychological, physical, economic or reputational harm	A person is physically harmed, has property damaged, or experiences psychological distress as a consequence of an AI system, e.g. an automated vehicle failing to detect and killing a pedestrian, or automation bias resulting in wrong dosage in clinical trials.
Breach of privacy	Personally identifiable information of employees, consumers or citizens which is used by an organisation for AI training and deployment is collected, accessed or used unlawfully, or maliciously accessed or inadvertently disclosed without authorisation.

1. 215 strategic business decision makers were surveyed by HTI in December 2022.
2. See CEDA (2021) AI Principles to Practice

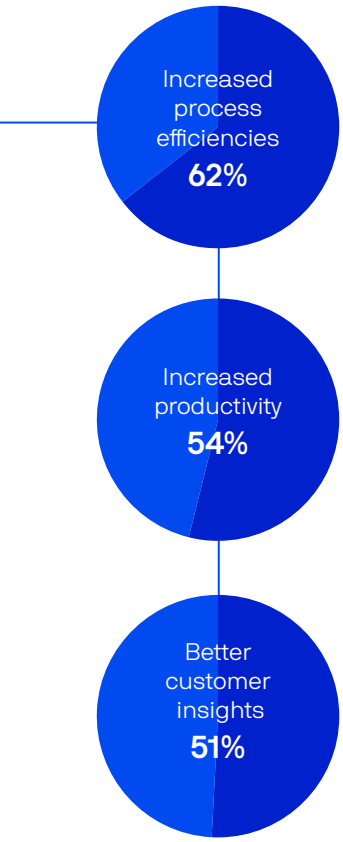
Growing risks to organisations fall into three categories

Organisations deploying AI face commercial, reputational and legal risks. Effective governance systems and tools are required by organisations striving to reap the benefits of responsible innovation, while discharging their legal obligations.

Risks to organisations

Commercial	Reputational	Legal
Commercial losses due to poor AI system performance, or adversarial attacks.	Damage to reputation and loss of trust due to harmful or unlawful treatment of consumers, employees or citizens.	Breach of legal and compliance obligations.

The greatest expected benefits of AI identified by decision makers were:



Company directors have critical duties to discharge in a context of growing AI use

Directors are responsible for ensuring that effective risk management and compliance systems are in place to discharge their directors' duties and associated responsibilities – including regarding any risks and impacts associated with a company's use of AI. To discharge duties when companies are using AI, directors should understand the external legal and regulatory environment that applies to their company and its use of AI (see Figure 2).

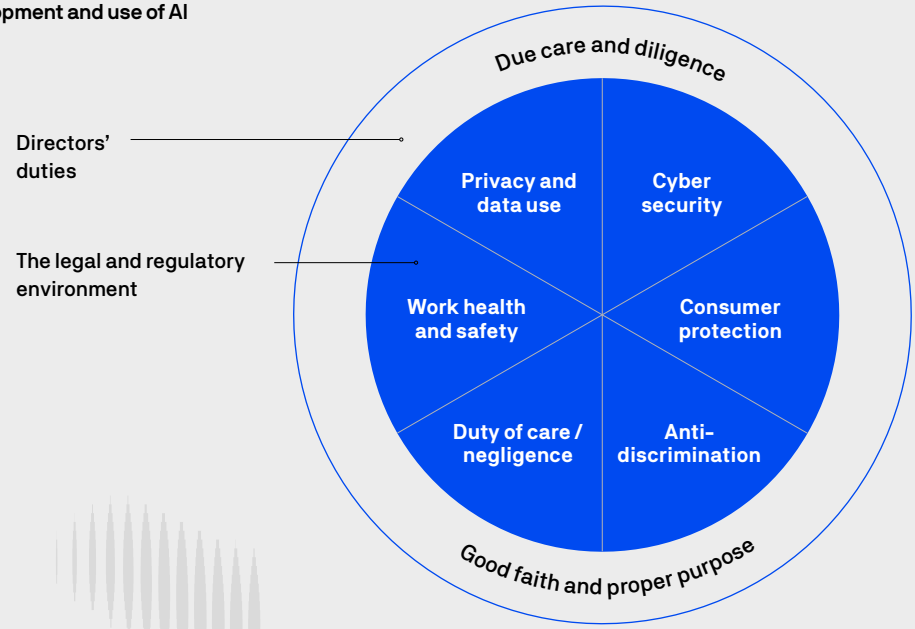
Directors' duties

Directors have a fiduciary duty to act in the best interests of the company. Directors, when making decisions and providing oversight regarding their company's development and use of AI systems, are required to act with independent and informed judgement, and exercise their powers and discharge their duties in accordance with the Corporations Act 2001 (Cth), which includes acting:

- With due care, and diligence
- In good faith, and for a proper purpose.

Focus is growing on the duty of care and diligence in the context of governance failures in meeting cyber security and privacy obligations,[3] which is a relevant consideration in the context of AI systems.

Figure 2: Key obligations in the design, development and use of AI



3. Teele Langford & Godwin (2021) Directors' duties and cyber security - it's complicated. Pursuit, University of Melbourne. https://pursuit.unimelb.edu.au/articles/directors-duties-and-cyber-security-it-s-complicated

Significant legal obligations apply to organisations using AI

While stand-alone AI regulation has not been introduced in Australia to date, a range of existing laws of general application apply to the design, development and use of AI systems. Some place obligations on the organisation as a whole, while others apply to directors and officers[4].

Privacy

Personal information (PI) is often collected and used to train and develop AI systems, or may be ingested in or used by a deployed AI system. Organisations need to consider their privacy obligations, which for those regulated by the *Privacy Act 1988* (Cth), includes the:

- open and transparent management of PI
- use and disclosure for only permitted purposes
- quality and accuracy (including of any PI outputs of AI)
- collection of PI only as reasonably necessary for an organisation's functions and with consent for sensitive information (including biometric information)
- notification of purpose for which PI is collected.

Consumer protection

Organisations engaging with consumers in the provision of AI-enabled products or services (including the provision of information or advice) are subject to *Australian Consumer Law* (ACL), including:

- prohibitions against unconscionable and misleading and deceptive conduct and false or misleading representations
- consumer guarantees (including that AI products are reasonably fit for purpose)
- liability for harm caused by safety defects (e.g. where organisation is a manufacturer under the ACL).

Duty of care / negligence

Organisations may have a general duty of care towards people that use or are impacted by an AI system. The law of negligence requires that where an organisation has a duty of care to a class of persons, the organisation:

- must exercise the standard of care of a reasonable person in the circumstances to avoid foreseeable injury or loss to the relevant persons
- may be liable for loss or injury suffered by those persons where the organisation fails to exercise that standard of care.

Cyber security

Cybersecurity is a key consideration for organisations that are developing and deploying AI, given the significant volumes of data involved and connectivity of AI systems. Obligations include:

- security, destruction and de-identification of PI, and notification of data breaches under the *Privacy Act 1988* (Cth)
- sectorial regulation, particularly for Australian financial services licensees and APRA-regulated entities, including various risk management and data security obligations
- reporting and other obligations for entities regulated by the *Security of Critical Infrastructure Act 2018* (Cth).

Anti-discrimination

The outputs of AI systems can directly or indirectly discriminate against individuals on the basis of protected attributes due to automated bias. Organisations have obligations under law[5], to prevent:

- discrimination based on a person's age, disability, disability carer status, sexual orientation, gender identity, intersex status, marital or relationship status, pregnancy status, breastfeeding or family responsibilities.

Work health and safety

Deployment of AI systems within a workplace context can introduce risks of physical and psychological harm to employees. Work, health and safety (WHS) laws require that:

- organisations ensure, as far as reasonably practical, the health and safety of workers and other persons, including factoring AI into health and safety training
- directors must exercise due diligence to ensure organisations meet their WHS obligations.

4. We note that this analysis is not comprehensive in nature, additional obligations apply to organisations based on industry, sector (e.g. the public sector), AI use case, or based on the organisation's business activities in non-Australian jurisdictions. **5.** Including the Racial Discrimination Act 1975, Sex Discrimination Act 1984, Disability Discrimination Act 1992 and Age Discrimination Act 2004 and other state and territory law

The Human Technology Institute is building a future that applies human values to new technology, helping organisations develop the skills, policies and tools to support the responsible development and use of emerging technologies.

For more information

Human Technology Institute
hti@uts.edu.au

University of Technology Sydney
PO Box 123
Broadway NSW 2007

uts.edu.au